



This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

DARK PATTERNS IN E-COMMERCE: A THREAT TO CONSUMER RIGHTS

~Jashandeep Kaur

INTRODUCTION

In today's era, online shopping is prevalent. When we open a shopping app to buy something and place an order, the bill, the cart shows an added travel insurance for which nobody asked, along with a countdown clock that says the deal expires in a few minutes, and other people are looking for the same product right now. This does not happen by accident or coincidence. In such apps, every design choice is properly tested, measured, and developed to increase sales.

Happening of such circumstances can be referred to as dark patterns. The Guidelines for the Prevention and Regulation of Dark Patterns define dark patterns as deceptive design techniques that manipulate the user interface (UI) or user experience (UX) and are employed on online platforms. These techniques manipulate the user into taking actions which they did not intend or voluntarily choose. These practices influence consumers' decisions and hence interfere with their autonomy in decision-making. These practices violate consumer rights and lead to unfair trade practices. So, the dark patterns are tricks built into the websites and apps that confuse and pressure a person into a decision they did not really want to make.¹

Harry Brignull, who was a user experience designer, coined the term 'dark patterns' in 2010. He described how interfaces are deliberately designed to pull the wool over consumers' eyes and trick them into actions they did not intend initially, for example, buying insurance with a purchase or signing up for recurring bills.² Now, after fifteen years, these dark patterns have become the centre for a large part of the internet to make money, and hence, they are not just a

¹ *Guidelines for Prevention and Regulation of Dark Patterns, 2023*, F. No. J-25/2/2023-CPU, Central Consumer Protection Authority ¶ 2(e) (Nov. 30, 2023)

² Neha Kapoor, *Dark Patterns in Digital Platforms: India's Rules & Guidelines*, Neeti Niyaman (Sept. 2025), <https://neetiniyaman.com/dark-patterns-digital-platforms/> (last visited July 18, 2026).

fringe design habit. This article looks at what dark patterns are, why they are linked to consumer rights, what the response of Indian and foreign law is, and what needs to be done.

WHAT IS A DARK PATTERN?

India's Central Consumer Protection Authority (CCPA) defines a dark pattern as any practice or deceptive design pattern which uses user interface or user experience choices on a platform that is built to mislead or trick a user into doing something they did not originally mean to do.³

The definition looks complex, but the idea behind it is simple. A shopping website is not neutral, but it provides a preference to some products over others. A website is designed by someone with proper buttons, colour, words, and pops up on the screen, and the designer usually aims to maximise the business. Although most of the design work does not harm any consumer, it is done to provide help. Such as a well-defined search bar or buttons like 'buy now', make shopping easier. A dark pattern comes into existence if such a design does not help the user to decide what they want, instead overriding their decision with pressure, confusion or irrelevant or unrevealed information.

Dark patterns are different from normal marketing practices. Dark patterns are not persuasive but manipulative in nature. The objective of dark patterns is to make consumers give up their own choices and act in a way inconsistent with them. In the case of ordinary marketing, if there is a misleading advertisement, then the consumer can question it, but in dark patterns, the interface itself commits the deception. A dark pattern is embedded into the mechanism of the page, such as a countdown timer that resets with every reload; the button for subscription is big, bright and clearly visible, but the button to cancel subscription is often small, grey and not clearly visible on the page. Such kind of tactics never allow the user to know that their choices and preferences are altered by the page of dark patterns.

COMMON TYPES OF DARK PATTERNS

In November 2023, the Guidelines for the Prevention and Regulation of Dark Patterns, 2023, were notified by the CCPA. These guidelines give a list of thirteen recognised dark patterns which are used in e-commerce and digital platforms across India. The list includes types such as false urgency, basket sneaking, confirmed shaming, forced action, subscription traps,

³ Guidelines for Prevention and Regulation of Dark Patterns, 2023, cl. 2, F. No. J-24/34/2023-CPU (Reg.) (India),

<https://consumeraffairs.nic.in/sites/default/files/The%20Guidelines%20for%20Prevention%20and%20Regulation%20of%20Dark%20Patterns%2C%202023.pdf>.

interface interference, bait and switch, drip pricing, disguised advertisement, nagging, trick wording, Saas billing, and rogue malware.⁴

In fake urgency, there is the use of a fake countdown clock, or claims are made that the stock is running low or there are only limited articles, but these claims are not true. The purpose of these false claims is to create an urgency in the mind of the consumer so that he places an order quickly without comparing prices elsewhere. In basket sneaking, there is the addition of an extra item, donation or service to the cart. This is all done without the proper consent of the shopper. The offers, like insurance plans or warranty slips, are added at the time of checkout. Confirm shaming uses guilt-inducing language on the option that a business does not want to be chosen, such as a pop-up asking a user to sign up for a discount with a decline button that says 'no thanks, I like paying full price'. Drip pricing refers to showing extremely low prices at first instance, but at the time of final checkout, delivery fees, service charges or taxes get added, and the consumer has invested the time in the process, and hence he is less likely to go away. In subscription traps, it is very easy and simple to sign up, and it can often be done through a trial process. But when it comes to cancellation, the cancel option is buried under several screens or hidden menus and can even require several phone calls. Interface interference uses visual design, colour, or placement to highlight the option that is beneficial for the seller and to bury the option that is advantageous for the consumer. Nagging refers to repeated interruptions that ask a user to do something, such as turn on the notification. These interruptions keep on going until the consumer gives consent out of frustration. Trick wording includes the use of confusing or double-meaning words so that the consumer agrees to something which they would have denied if plain or normal language were used.

All these tricks can be used together to mislead consumers. A single checkout page can contain a countdown timer, drip prices, a guilt-based decline button, etc. Each element on its own seems a small nudge, but together they lead to an engineered choice by the consumer and huge profit to the business.

WHY DARK PATTERNS ARE AGAINST CONSUMER RIGHTS

The basic idea behind the consumer protection law is that the thing purchased by the consumer should reflect his free and informed choice. But dark patterns are a precise and direct attack on

⁴ Press Info. Bureau, Ministry of Consumer Affairs, Food & Pub. Distrib., *E-Commerce Platforms Urged to Self-Audit and Eliminate Dark Patterns: Centre* (July 22, 2025), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2146813>

this idea. Dark patterns take advantage of the predictable weaknesses in human decision-making and exploit human attention. Although dark patterns do not put a gun on buyers' heads to buy something, they use schemes which cause the buyer to trust a default option. The buyer can feel discomfort from being judged or anxious because of the ticking clock. The consent of the consumer does not remain free when the checkout system is designed by exploiting such weaknesses.

This led to financial harm as well as harm to autonomy and trust. The financial harm is real and the most significant harm. The financial harm can involve unwanted subscriptions, hidden or unrevealed fees, or non-refundable add-ons purchased by mistake. Harm to trust and autonomy occurs when the consumer finds out that the shopping app has been secretly and quietly manipulating his choices for months. After discovering this, the consumer is unlikely to trust that app or digital commerce again in the same way. Hence, the increasing use of dark patterns can reduce public confidence in online markets. And the loss would be suffered by honest businesses and consumers.

A certain category of population is more vulnerable to this harm than others. For example, elderly users, first-time internet shoppers, and people who are less familiar with digital interfaces are more exposed to this harm. Their probability of recognising such manipulative designs is lower, and they can be trapped easily. As these design tricks work below the level of conscious awareness, the advice of caveat emptor to read carefully before buying is a weak defence. The entire motive of the dark pattern is to defeat careful reading.

RESPONSE OF THE INDIAN LEGAL SYSTEM

Consumer Protection Act 2019, the Consumer Protection (E-commerce) Rules, 2020 and the Guidelines for Prevention of Misleading Advertisements and Endorsement of Misleading Advertisements 2022 were the main laws for deceptive design. Dark patterns were indirectly addressed through these laws before the existence of the special laws. These instruments treated deceptive design as a form of unfair trade practice or misleading advertisement instead of a distinct category of harm.⁵

Later, the CCPA recognised that this indirect application of laws is not enough to take down the specific mechanism of digital manipulation. Then, the CCPA acted under section 18 of the Consumer Protection Act 2019 and issued guidelines for the Prevention and Recognition of

⁵ Kapoor, *supra* note 1.

Dark Patterns 2023 on November 30, 2023. The draft was released on September 7, 2023, and then, after consultation with the stakeholders, the guidelines were released in November.⁶

The 2023 guidelines apply to all platforms which systematically offer goods and services in India. These guidelines are also applicable to foreign platforms which are providing their services to Indian customers. The sellers and advertisement which are operating on these platforms also fall under the ambit of these guidelines. It is also clarified in the guidelines that these guidelines do not replace any existing law which already regulates dark patterns. The guidelines are applicable in addition to any existing laws or regulations.⁷

The enforcement of these guidelines has continued to evolve. In June 2025, the CCPA issued an advisory, and it became effective on the following day. The CCPA exercised section 18(1) of the 2019 Act, and it directed all e-commerce platforms to conduct a self-audit of their interfaces within the time period of three months. The platforms are directed to identify any of the thirteen listed dark patterns in use and implement corrective measures. This is directed to make consumer interaction fair, ethical and transparent.⁸ The advisory put emphasis on Rule 4(9) of the Consumer Protection (E-Commerce) Rules, 2020. This rule states the requirement of consent of the user through a clear and affirmative act rather than through default settings or silence.⁹

But there are some weaknesses and shortcomings in the 2023 Guidelines and the 2025 Advisory. Commentators have pointed out that these guidelines and advisory majorly relies on self-regulation and self-audits. There is limited clarity on penalties for any specific violation and how seriously the CCPA will investigate the platforms which do not comply with such guidelines and advisory. As the guidelines are issued under section 18, they have the authority of the parent Act. The CCPA have general power to investigate unfair trade practices and can impose a penalty only under the 2019 Act. There is an absence of a specialised penalty schedule behind each of the thirteen listed patterns, and hence it allows platforms to treat compliance as an option until a specific complaint is raised.

Along with consumer protection law, the Digital Personal Data Protection Act, 2013 is also relevant. This Act adds a complementary layer to dark patterns that manipulate consent for data

⁶ Internet Freedom Found., *Dark Patterns: Comments on the Draft Guidelines for Prevention and Regulation of Dark Patterns* (Oct. 2023), <https://internetfreedom.in/>.

⁷ Guidelines for Prevention and Regulation of Dark Patterns, 2023, cls. 3, 6, *supra* note 3

⁸ Internet Freedom Found., *Dark Patterns and Weak Remedies: Why the CCPA Advisory Falls Short* (June 23, 2025), <https://internetfreedom.in/dark-patterns-and-weak-remedies-why-the-ccpa-advisory-falls-short/>.

⁹ *Id.*

collection. This Act helps in reducing pre-ticked boxes and confusing consent banners on which the dark patterns rely by requiring consent for processing personal data to be free, informed and given through a clear affirmative act.

THE GLOBAL PICTURE: COMPARISON WITH THE UNITED STATES

Over the past years, the Federal Trade Commission (FTC) in the United States has taken dark patterns very seriously. The FTC is empowered by Section 5 of the Federal Trade Commission Act to protect consumers and ensure a fair market. So, the FTC uses the authority given by this section. Along with this provision, there is also another legislation named the Restore Online Shoppers' Confidence Act (ROSCA). This act specifically governs negative option and subscription billing.

The FTC issued an enforcement policy statement in 2021. It has warned businesses that they must disclose material terms clearly while asking for a subscription or sign-up. They must obtain express and informed consent. Businesses are required to offer a subscription cancellation process as easy as signing up.¹⁰

In 2023, it sued Amazon.com, Inc for allegedly trapping users in Prime subscriptions through a deliberately confusing cancellation process. The court proceeded with the case in 2024, and it ended in a major settlement.¹¹ The other platforms, like Epic Games, Credit Karma and Adobe, have also faced similar penalties for manipulative interface designs. These cases set an example that sustained enforcement against powerful platforms can result in a real design change.

SUGGESTIONS

India's 2023 guidelines were a strong step towards dark patterns. Previously, there were only vague unfair trade practice standards, but these guidelines provided thirteen dark patterns. But the CCPA has relied on voluntary self-audits, and hence the guidelines are not binding. Compliance remains largely voluntary, and public awareness of these rules remains low.¹²

These regulations should attach real penalties to the self-audit process. Strict regulations are still required in India, as the regulatory pressure can change the behaviour of the platforms.

¹⁰ Coulson P.C., *Dark Patterns Lawsuits and the FTC's Click-to-Cancel Rule* (Oct. 14, 2025), <https://www.coulsonpc.com/coulson-pc-blog/dark-patterns-ftc-click-to-cancel-rule>.

¹¹ Complaint at 1–3, *FTC v. Amazon.com, Inc.*, No. 2:23-cv-00932 (W.D. Wash. filed June 21, 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/2123050-amazoncom-inc-rosca-ftc-v>.

¹² Guidelines for Prevention and Regulation of Dark Patterns, 2023, *supra* note 3.

Only identification of the problem is not sufficient. Real enforcement and an informed public are required to make these guidelines and regulations meaningful. For this, CCPA needs transparent records of enforcement, which include published data about the number of audited platforms, how many violations were found and what penalties followed. There should be consumer awareness campaigns, and these campaigns should be conducted in the language understood by the consumers. The government, consumer court, law schools or civil society should conduct these campaigns periodically. India can learn from the American model of enforcement on how it forced Amazon to redesign the Prime Cancellation flow.

There is no need for a new legal theory; the only thing required is institutional will. The consent to purchase should be real. The consent should not be altered or manufactured through design tricks. This principle already exists in law. The only thing pending is enforcement. Consumer education should be a must, and there should be a proper solution to resolve and treat the violations seriously as any other consumer fraud.¹³

CONCLUSION

At the end, addressing dark patterns is about maintaining the integrity of digital markets and ensuring that technology serves the consumer rather than exploiting them. As more people depend on online platforms for shopping and other day-to-day services so it should be the moral duty of businesses to focus on being transparent instead of relying on confusing and misleading practices. Laws and guidelines can only be effective if they are properly implemented and consumers are aware of their rights. A fair digital market is one where trust is earned through honest practices, not through manipulation. Strengthening the trust is beneficial for both the consumer as well as the businesses in the long run.

¹³ Coulson P.C., *supra* note 10.